REMARKS

Applicant hereby responds to the Office Action of August 10, 2005 in the above-referenced patent application. Claims 1, 3-8 and 10-41 are pending in the patent application, of which claims 15-41 were withdrawn from consideration. As such, Claims 1, 3-8 and 10-14 are under consideration.

Claims 1, 3-8 and 10-14 were rejected under 35 U.S.C. 103(a) as being unpatentable over USPN 5,809,139 to Girod et al. (hereinafter "Girod") in view of USPN 5,742,685 to Berson et al. (hereinafter "Berson"). Rejection of the claims is respectfully traversed because the references, alone or in combination, do not disclose or suggest all of the limitations of the claims.

Interview Summary

Applicant wishes to thank the Examiner for the telephonic interview of November 1, 2005 with Applicant's representative, Michael Zarrabian (Reg. No. 39,886), in which rejection of Claim 1 under 35 U.S.C. 103(a) as being unpatentable over Girod in view of Berson was discussed. Applicant provided arguments based on the following arguments/remarks, and agreement was reached with the Examiner that the cited references do not disclose all of limitations of Claim 1 (i.e., Berson and Girod do not teach limitation (d) of Claim 1), whereby no

prima facie case of obviousness has been established.

Applicant further brought to the attention of the Examiner that Applicant believes limitations of Claim 1 are novel and non-obvious, such as for example, limitation (d) of transmitting *the scrambled signal and said data signal to a receiver* for subsequent recovery of said scrambled signal.

Arguments/Remarks

For completeness, Applicant further provides the following arguments/remarks in support of allowance of the claims.

As per **Claim 1**, it is respectfully submitted that Girod does not teach all of the claimed limitations, and despite the Examiner's interpretation, Berson does not disclose the claimed limitations that are not disclosed by Girod. According to Claim 1, the present invention provides a system for copy protecting a digital signal representing audiovisual information. The audiovisual digital signal is first encoded to obtain an encoded signal, and the encoded signal is converted into a copy protected signal using a copy protection function (the copy protection function utilizes a CP data signal representing copy protection data). Then the copy protected signal is scrambled to obtain a scrambled signal, and the scrambled signal and said CP data signal are transmitted to a receiver.

In Berson, a person whom the identification card will identify, is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding, which is incorporated into one portion of the identification card. The signal representing the image is encrypted using a public key encryption system and the key is downloaded from a center. To validate the card the coded message is scanned, decoded, decrypted, expanded and displayed. (Abstract).

However, Berson does not teach the limitations of "transmitting the scrambled signal and said data signal to a receiver for subsequent recovery of said scrambled signal," as required by Claim 1. According to the claimed invention, an encoded signal that is copy protected with copy protection data and then scrambled, is transmitted to the receiver along with the copy protection data signal. The scrambled signal is generated by encoding a digital signal to obtain an encoded signal, converting the encoded signal into a copy protected signal using a copy protection function, wherein the function utilizes a data signal representing copy protection data, and scrambling the copy protected signal to obtain a scrambled signal, as required by Claim 1.

According to Berson an encryption key E_i and an encoded decryption key $X[D_i]$ are transferred from center 40 to the encrypter module 20. However, nowhere in Berson are the limitations of transmitting the scrambled signal and said data signal to a receiver for subsequent recovery of said scrambled signal, according to Claim 1, taught or suggested.

In addition, the Examiner again asserts that: "Yet a careful reading of Berson reveals that such is indeed taught by Berson by virtue of the step of Berson wherein encrypted data Ei[M] and an encoded decryption key X[Di] are transmitted to printer module (fig. 1 item 28) which does constitute a receiver for the information." Applicant respectfully traverses the Examiner's assertion.

Not only is item 28 never referred to or mentioned in the description of Berson, but item 28 in Fig. 1 of Berson is designated a printer, not a receiver for subsequent recovery of said scrambled signal. Despite the Examiner's assertion above, there is no disclosure or suggestion in Berson that encrypted data Ei[M] and an encoded decryption key X[Di] are even transmitted to item 28.

The Examiner states that: "In response to this the Examiner notes that Berson mistakenly references the printer, item 28 in fig. 1, as item 20 in col. 1, lines 50-55. Despite this typographical error, it is cleat that item 28 'Printer' is being referenced by virtue of it being referred to as "Printer" and its functionality described as production ('Printing') of an identification card." (Office Action, Page 3, first full paragraph). The Examiner further states that Berson teaches transmission of a scrambled signal and a data signal to a receiver for subsequent recovery of said scrambled signal in fig. 1 item 28 where encrypted data Ei[M] and

an encoded decryption key X[Di] are transmitted to a printer module which constitutes a receiver for the information. (Office Action, Page 6, first full paragraph).

However, in col. 1, lines 50-55 of Berson (relied on by the Examiner), there is no reference to item 28 or item 20. At any rate, in fig. 1 of Berson, the only connections to item 28 are from the output of module 30 and the output of A/D 14. The A/D 14 provides a digital signal of a user's identification card (Berson, col. 3, lines 10-17), and the text input 30 provides a text message T such as a user's identification (Berson, col. 3, lines 57-60). Accordingly, Berson does not disclose or suggest anywhere that encrypted data Ei[M] and an encoded decryption key X[Di] are transmitted to item 28 or a printer module for subsequent recovery of said scrambled signal.

Indeed, in col. 3, lines 50-55, Berson states that: "The digitized first signal is also input to printer 20 which may use any appropriate technology for the production of identification card C to print an image of person P on front CF of identification card C. Front CF and back CB are then combined and laminated using well known technology by laminator 32 to product identification card C." As such, even if item 20 is a printer as the Examiner states, nevertheless the only connections to printer are from the output of module 30 and the output of A/D 14, and not the encrypted data Ei[M] and an encoded decryption key X[Di] for subsequent recovery of said scrambled signal, as claimed herein. Where is that disclosed in Berson?

Accordingly, Berson does not disclose the limitations of: "(d) transmitting the scrambled signal and said data signal to a receiver for subsequent recovery of said scrambled," according to Claim 1, wherein the scrambled signal was generated by encoding a digital signal to obtain an encoded signal, converting the encoded signal into a copy protected signal using a copy protection function, wherein the function utilizes a data signal representing copy protection data, and scrambling the copy protected signal to obtain a scrambled signal, as required by Claim 1.

The Examiner states that motivation for combining Girod and Berson is provided in Girod, col. 1, lines 50-60, and that including Girod's frequency-spreading signal with the transmitted data of Berson would facilitate rapid recovery of the watermark signal. However, as discussed the references, alone or in combination do not disclose all of the claimed limitations. Further, even if including frequency-spreading into Berson provides rapid recovery of a watermark, that has nothing to do with the claimed limitations. In addition, the Examiner has not explained how placing frequency-spreading into Berson provides rapid recovery of a watermark.

More importantly, the Examiner modifies Berson with teachings of Girod, without citing any motivation in *Berson* to be modified as suggested by the Examiner. Indeed, Berson mentions nothing about speeding up verifying an identification card and recording verification of the card. Nor had the Examiner explained how the frequency-spreading technique of Girod can be

included in Berson to provide a functioning system, and without major modifications that are not obvious to one of the art.

It is well settled that in order for a modification or combination of the prior art to be valid, the prior art itself must suggest the modification or combination, "...invention cannot be found obvious unless there was some explicit teaching or suggestion in the art to motivate one of ordinary skill to combine elements so as to create the same invention." *Winner International Royalty Corp. v. Wang*, No. 96-2107, 48 USPQ.2d 1139, 1140 (D.C.D.C. 1998) (emphasis added). "The prior art must provide one of ordinary skill in the art the motivation to make the proposed molecular modifications needed to arrive at the claimed compound." *In re Jones*, 958 F.2d 347, 21 USPQ.2d 1941, 1944 (Fed. Cir. 1992) (emphasis added). Neither of the references suggests the motivation to modify or combine the references as proposed. Berson are individually complete and functionally independent for their limited specific purposes and there would be no reason to make the modification proposed by the Office Action. Because neither of the prior art references suggests the combination and modifications proposed by the Office Action the combination and modifications are improper. For at least these reasons, rejection of Claim 1 should be withdrawn.

Further, in col. 3 line 57 to col. 4, line 25 (relied on by the Examiner), Berson states that:

> "Text input 30 provides text message T and at least a portion of text message T, which preferably includes other personal information such as name, address, license number, etc. relating to person P, is combined with the compressed form of the first signal to form the second signal which is encrypted by encrypter module 20 to provide encrypted information $E_i[M]$.... [L]ike image I text T is embodied in card C in both humanly recognizable form on the front CF and coded and encrypted form on the back CB of card C. In a preferred embodiment of the subject invention a data center 40 transmits encryption code E_i to encrypter module 20.... To facilitate decryption of encrypted information $E_i[M]$ data center 40 also transmits an encrypted decryption key $X[D_i]$ to be appended to the encrypted information $E_i[M]$ by coder module 22... [W]hen card C is to be verified the necessary decryption key D_i can be obtained by decrypting encrypted decryption key $X[D_i]$...." (emphasis added).

According to Berson, the image I and text T are embodied in card C in both humanly recognizable form on the front CF of the card, and coded in encrypted form on the back CB of card C. In the preferred embodiment of FIG. 1, the data center 40 transmits encryption code E_i to the encrypter module 20. For later decryption of encrypted information $E_i[M]$, the data center 40 also transmits an encrypted decryption key $X[D_i]$ to be appended to the encrypted information

$E_i[M]$ by coder module 22. When later the card C is to be verified, the necessary decryption key D_i can be obtained by decrypting encrypted decryption key $X[D_i]$. Therefore, the data center 40 sends encryption key E_i and decryption key D_i to the encrypter module 20, such that the encrypted information $E_i[M]$ and decryption key D_i are placed on the card for later validation of the card.

As such, in Berson data center 40 sends encryption key E_i and decryption key D_i to encrypter module 20, such that the encrypted information $E_i[M]$ and decryption key D_i are placed on the card for later validation of the card. By contrast, according to the present invention, an audiovideo digital signal is first encoded to obtain an encoded signal, and the encoded signal is converted into a copy protected signal using a copy protection function (the copy protection function utilizes a CP data signal representing copy protection data). Then the copy protected signal is scrambled to obtain a scrambled signal; and the scrambled signal and said CP data signal are transmitted to a receiver.

FIG. 2 of Berson shows apparatus 50 for validating the identification card C. The back CB of card C is scanned by a barcode scanner 52 having the capability to scan an appropriate two dimensional barcode. The scanned signal is then decoded by decoder module 54 and decrypted by decrypter module 58. Key X (or keys) is obtained by decrypter 58 from center 40. According to Col. 4, lines 9-12 of Berson, the data center 40 does not send out copy protected, encrypted

information, AND a data signal to be used to remove the copy protection. The data center only provides encryption and decryption keys to encrypter 20. This is totally different than the present invention.

By contrast, the present invention provides a system for copy protecting a digital signal representing audiovisual information, including the limitations of "transmitting the scrambled signal and said data signal to a receiver for subsequent recovery of said descrambled signal," as required by Claim 1. The audiovisual digital signal is first encoded to obtain an encoded signal, and the encoded signal is converted into a copy protected signal using a copy protection function (the copy protection function utilizes a CP data signal representing copy protection data). Then the copy protected signal is scrambled to obtain a scrambled signal, and the scrambled signal and said CP data signal are transmitted to a receiver. There is no such teaching in Berson.

Further, Applicant respectfully maintains that Berson is non-analogous art and not reasonably pertinent to the present invention because Berson is directed to an identification card and a system for producing and authenticating such an identification card. According to Berson, a person whom the identification card will identify, is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding, which is incorporated into one portion of the identification card. The signal representing the image is encrypted using a public key encryption system and the key is

downloaded from a center. To validate the card the coded message is scanned, decoded, decrypted, expanded and displayed. (Abstract). Despite the Patent Office's interpretation, Berson is not in the field of the invention. For example, as discussed, Berson is not even related to protecting a transmitted signal from illicit use. For at least these reasons, rejection of Claim 1, and all claims dependent therefrom, should be withdrawn.

As per **Claim 3**, for example, the limitation of "transmitting the scrambled signal and said data signal as a single signal" is not disclosed or suggested by the references, alone or combination, for reasons provided in relation to Claim 1. Berson does teach such a limitation.

As per **Claim 4**, the limitation of "combining the scrambled signal and said data signal into said single signal" is not disclosed by the references, alone or combination, for reasons provided in relation to Claim 1. If Claims 3 and 4 are again rejected, Applicant respectfully requests that the Examiner refer to such specific limitations in the references, if they exist, and provide specific reasons for rejection of each claim.

As per **Claim 6**, according to Claim 1 on which Claim 6 is dependent, initially a digital signal is copy protected by: (a) encoding the digital signal to obtain an encoded signal; (b) converting the encoded signal into a copy protected signal using a copy protection function, wherein the function utilizes a data signal representing copy protection data; (c) scrambling the

copy protected signal to obtain a scrambled signal; and (d) transmitting the scrambled signal and said data signal to a receiver. The present invention offers the flexibility of using copy protection data to introduce copy protection, and then use the transmitted copy protection data, to recover/remove the copy protection, according to Claim 6.

Girod does not disclose "descrambling the scrambled signal to recover said copy protected signal", as required by Claim 6. Girod does not disclose "reconverting the recovered copy protected signal back into the encoded signal using an inverse copy protection function, wherein the inverse function utilizes copy protection data from said copy protection data signal", as required by Claim 6. Girod does not disclose "decoding the converted encoded signal to recover said digital signal," as required by Claim 6.

By contrast, in relation to Figure 1 (relied upon by the Patent Office), Girod states:

> "The input to the system is either a digital video signal or an analog video signal..." (col. 3, lines 49-52);
>
> "The digital video signal (either original or converted using A/D converter 8) is then input to a video coder 10, which is one of a number of different known digital video compression coders" (col. 3, lines 55-58); and
>
> "Referring again to FIG. 1, the output of the interframe coder 10 is input to either digital watermarking apparatus 26 or data storage device 24" (col. 4, lines 60-62).

Then in conjunction with Figures 1 and 2c, in col. 5, lines 7-10 of Girod (*relied upon by the Examiner*), Girod states:

> "Once the signal is watermarked, it is transmitted to the receiver in question. The received signal can then be decoded at the destination site using interframe video decoder 28. The decoder 28 performs the inverse functions of the coder 10, in a manner well understood in the art. The watermark, having been embedded in the digital signal, can be recovered later in a manner described below."

Clearly, in Figures 1 and 2c and col. 5, lines 7-10, Girod does not disclose "descrambling the scrambled signal to recover said copy protected signal", as required by Claim 6. Further, Girod does not disclose "reconverting the recovered copy protected signal back into the encoded signal using an inverse copy protection function, wherein the inverse function utilizes copy protection data from said copy protection data signal", as required by Claim 6. Recovering copy protection data allows use of that data by a reconverter to reconvert the copy protected signal. Indeed, Girod does not disclose an inverse copy protection function that utilizes copy protection data from the copy protection data signal provided by a transmitter. And, Girod does not disclose "decoding the converted encoded signal to recover said digital signal," as required by Claim 6. The Patent Office is reading steps of the claimed invention into Girod, and as is clear from above, those steps do not exist in Girod.

The Examiner further states that in col. 5, line 49 to col. 6, line 17 Berson teaches reconverting the recovered copy protected signal back into the encoded signal using an inverse copy protection function, wherein the inverse function utilizes copy protection data from said copy protection data signal, as required by Claim 6. However, there is absolutely no such disclosure in Berson, and indeed the passage in col. 5, line 49 to col. 6, line 17 of Berson has nothing to do with the claimed limitations. Indeed, in col. 5, line 49 to col. 6, line 17 Berson states:

> Turning to FIG. 3, secure verification transaction record 90 is shown. Record 90 includes source identification 92, which is preferably machine number 80 or similar identification of the source of the record, and time 96, which is preferably provided by secure clock 84 so that the system operator or a third party cannot falsify the time at which the verification transaction took place. Record 90 also includes decrypted text 98 which includes at least personal information relating to person P whose identify is being verified. In a preferred embodiment of the subject invention record 90 also includes decrypted image 100 from decrypter 58 and new image 102 from scanner 72 and transaction information 104 from input 76. Record 90 is then electronically notarized by appending digital signature 108 in a conventional manner. Generally, electronic notarization includes appending secure time information to a message and then digitally signing the message to

provide assurance that the message was recorded at that particular time. Such electronic notarization is known and is described in U.S. patent number in U.S. Pat. No. 5,022,080; to: Durst et al.; issued: Jun. 4, 1991, which is hereby incorporated by reference. Other methods (such as digitally signing a document to which information derived from previous documents in a stream of documents has been appended so that the position of the document in the stream of documents is established) for securely establishing the time of recording and content of a message are known and are included within the meaning of the term "electronic notary" as used herein. In another preferred embodiment of the subject invention data processor 110 accesses database store 86, using conventional database access the techniques, to generate various reports of verification transactions. For example in a liquor store application data processor 110 might generate specialized customer mailings. Or reports 112 of access by particular persons or during particular time periods can be printed by printer 116 to provide an audit trail of verification activity.

Applicant requests that the Examiner quote specific language in the above passage where Berson discloses each an everyone of the five limitations in Claim 6: (1) a copy protected signal, (2) reconverting the recovered copy protected signal, (3) reconverting the recovered copy protected signal back into the encoded signal, (4) reconverting the recovered copy protected

signal back into the encoded signal using an inverse copy protection function, (5) wherein the inverse function utilizes copy protection data from said copy protection data signal.

It is respectfully submitted that if the Examiner cannot provide such disclosure in Berson, the rejection of Claim 6 must be withdrawn. Therefore, for at least these reasons, Claim 6 should be allowed.

As per **Claims 5, 7, 12 and 14**, at least the limitations in parts (a)-(d) of Claim 5, parts (a)-(e) of Claim 7, parts (a)-(d) of Claim 12, and parts (a)-(c) of Claim 14, are not taught or suggested by the references, alone or combination, for the above reasons. The Patent Office has not shown where these limitations are disclosed in the references. For at least these reasons and the reasons provided above, rejections of Claims 5, 7, 12 and 14 should be withdrawn. If Claims 5, 7, 12 and 14 are again rejected, Applicant respectfully requests that the Patent Office refer to such specific limitations in the references, if they exist, and provide specific reasons for rejection of each claim.

As per **Claim 8**, for the same reasons provided above in relation to Claim 1, rejection of Claim 8, and dependent claims therefrom, should be withdrawn.

As per **Claim 10**, the claimed limitations of a combiner for combining the scrambled

signal and said data signal into said single signal, and a transmitter for transmitting said single signal, are not disclosed or suggested by the references, alone or combination, for reasons provided in relation to Claim 1. If Claims 1o is again rejected, Applicant respectfully requests that the Patent Office refer to such specific limitations in the references, if they exist, and provide specific reasons for rejection of the claim.

As per **Claim 11**, the limitation of a transmitter for transmitting the scrambled signal and said data signal as a single signal, is not disclosed or suggested by the referenced, alone or in combination, for at least the reasons provided above item 28 in Fig. 1 of Berson in relation to Claim 1. If Claim 11 is again rejected, Applicant respectfully requests that the Patent Office refer to such specific limitations in the references, if they exist, and provide specific reasons for rejection of the claim.

As per **Claim 13**, the above arguments in relation to rejection Claim 6, are incorporated herein, in response to rejection of Claim 13. Therefore, for at least these reasons, Claim 13 should be allowed.

CONCLUSION

Please charge any additional fees or credit any overpayment to our Deposit Account No. 01-1960. A duplicate copy of this page is enclosed for this purpose.

Re-examination, reconsideration and allowance of all claims are respectfully requested.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MS Amendment Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

November 10, 2005.

By: Sarah A. Nielsen

Sarah A. Nielsen

Signature

Respectfully submitted,

11/10/5

Kenneth L. Sherman (Date)
Registration No. 33,783
Myers Dawes Andras & Sherman, LLP
19900 MacArthur Blvd., 11th Floor
Irvine, CA 92612
(949) 223-9600
(949) 223-9610 – Fax
Customer No.: 23386

R:\M-Z\SAM1 - KLS - Samsung Electronics, Korea\SAM1.PAU.58\07AMD-revised.doc